



U.S. Department of Energy

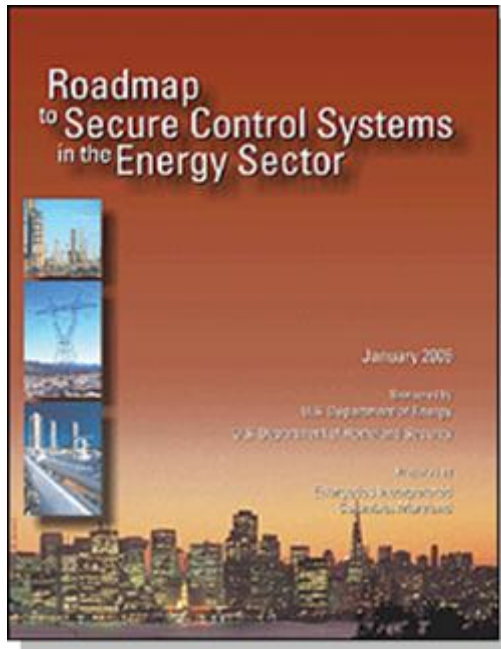
Office of Electricity Delivery and Energy Reliability

Working to Achieve Cybersecurity in the Energy Sector

“Cybersecurity for Energy Delivery Systems (CEDS)”

**Rita Wells
Idaho National Laboratory**

Roadmap – Framework for Public-Private Collaboration



- Published in January 2006
- *Energy Sector's* synthesis of critical control system security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
 - align activities to sector needs
 - coordinate public and private programs
 - stimulate investments in control systems security

Roadmap Vision

In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to **survive an intentional cyber assault with no loss of critical function.**

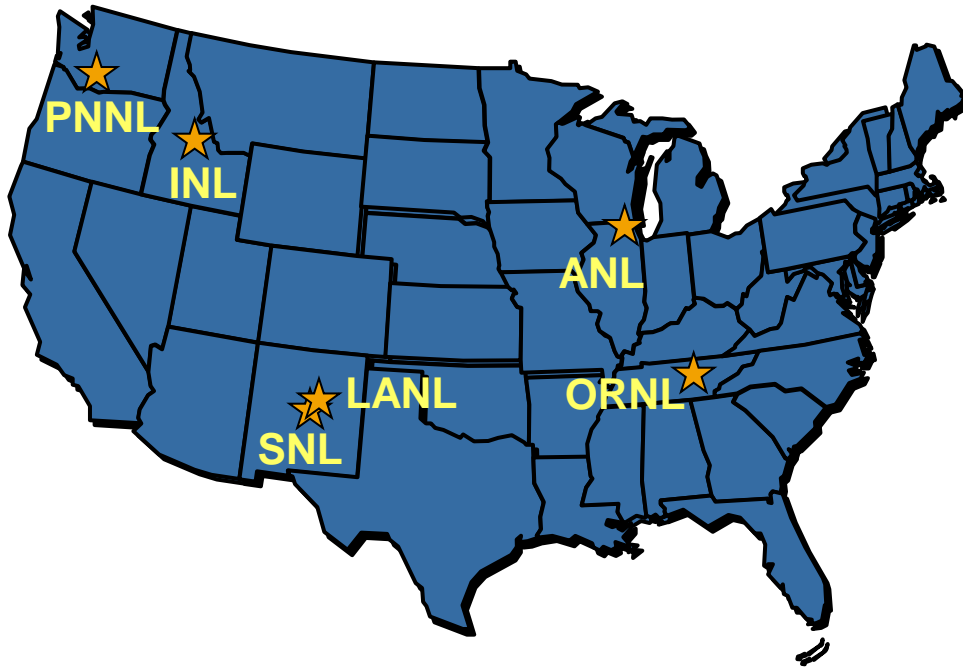
Roadmap – Key Strategies & 2015 Goals

Measure and Assess Security Posture	Develop and Integrate Protective Measures	Detect Intrusion & Implement Response Strategies	Sustain Security Improvements
Energy asset owners are able to perform fully automated security state monitoring and control systems networks with real-time remediation	Next-generation control systems components and architectures produced with built-in, end-to-end security will replace older legacy systems	Control systems networks will inform operator response to provide contingency and remedial actions in response to attempted intrusions	Implement effective incentives through Federal and state governments to accelerate investment in secure control system technologies and practices

DOE National SCADA Test Bed (NSTB) Program

DOE multi-laboratory program ...established 2003

Supports industry and government efforts to enhance cyber security of control systems in energy sector



Key Program Elements

- Cyber security assessments and recommended mitigations for energy control systems
- Integrated risk analysis
- Secure next generation control systems technology R&D
- Public-private partnership, outreach, and awareness

“..the only reliable way to measure security is to examine how it fails”

Bruce Schneier, Beyond Fear

17 NSTB Facilities From 6 National Labs

IDAHO Critical Infrastructure Test Range

- SCADA/Control System Test Bed
- Cyber Security Test Bed
- Wireless Test Bed
- Powergrid Test Bed
- Modeling and Simulation Test Bed
- Control Systems Analysis Center

SANDIA Center for SCADA Security

- Distributed Energy Technology Laboratory (DETL)
- Network Laboratory
- Cryptographic Research Facility
- Red Team Facility
- Advanced Information Systems Laboratory



PACIFIC NORTHWEST Electricity Infrastructure Operations Center

- SCADA Laboratory
- National Visualization and Analytics Center
- Critical Infrastructure Protection Analysis Laboratory



OAK RIDGE Cyber Security Program

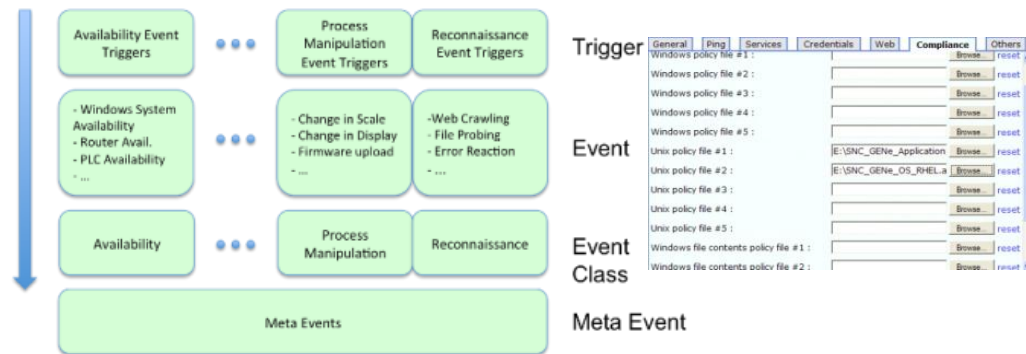
- Large-Scale Cyber Security and Network Test Bed
- Extreme Measurement Communications Center

ARGONNE Infrastructure Assurance Center

LOS ALAMOS Cybersecurity Program

2008 First DOE-Awarded Industry Projects

- **Hallmark Project - SEL**
 - Secure serial communication links
- **Cyber Security Audit and Attack Detection Toolkit - Digital Bond**
 - Baseline optimal security configuration
- **Lemnos Interoperable Security Program - EnerNex**
 - Interoperable configuration profiles and testing procedures



Trustworthy Cyber Infrastructure for the Power Grid

(TCIPG, University-Led Collaboration)

Vision: Architecture for End-to-End Resilient, Trustworthy & Real-time Power Grid Cyber Infrastructure

Smart-Grid – Enabled Load and Distributed Generation as a Reactive Resource

Katherine M. Rogers, *Student Member, IEEE*, Ray Klump, *Member, IEEE*, Himanshu Kharana, *Senior Member, IEEE*, Thomas J. Overbye, *Fellow, IEEE*

Abstract—At the residential level, devices which are in place now and expected in the future have the ability to provide reactive power support. Inverters which connect distributed generation such as solar panels and plug-in hybrid electric vehicles (PHEVs) to the grid are an example. Such devices are not currently utilized by the power system. We investigate the integration of these end-user reactive-power-capable devices to provide voltage support to the grid via a secure communications infrastructure. We show how to determine effective locations in the transmission system and how to control reactive power resources at these locations. We also discuss how to determine reactive support groups which parallel the regions of the secure communications architecture that is presented. Ultimately, our goal is to present how the Smart Grid can allow the utilization of available end-user devices as a resource to mitigate power system problems such as voltage collapse.

Index Terms— reactive power resources, cyber security, voltage control, linear sensitivity analysis

I. INTRODUCTION

Power system operation is currently contingency-constrained, and often by low-voltage violations. A contingency is a "what if" scenario that utilizes use to gauge the operational reliability of the power system. Utilities regularly run a series of contingencies in a process known as contingency analysis. Under normal conditions, the system is operated so that it can withstand the loss of any one element [1] or one credible contingency. The ability of a system to withstand a list of "credible" disturbances or contingencies is defined to be operational reliability, but was previously called security [2]. This means that for any single contingency, the steady-state analysis converges to a solution that can be enacted within an all state can be restored.

Currently, such at level. The Smart Grid paper, allows us to reactive power control transmission system's the idea of using as a devices which are can and discuss the need a secure communication system to maintain a power resources include hybrid electric vehicle sources [14], [15]. Lo converters are power resources for the grid

the effects of the outage can safely be assumed to be undesirable, perhaps leading to a voltage collapse. Voltage collapse is a process whereby voltages progressively decline until it is no longer possible to maintain stable operating voltage [3]. It is well known that available reactive power resources can be used system less vulnerable.

Optimal control to system to a stable control which focuses called corrective control to a new stable equilibrium [5], [6]. I out before any initial number of buses in it classified as severe the ramp limits of it restore the system, to one can choose real effective for the power switching of transmission corrective control [8] lines changes the system changes the system engineering field. Still, changing power supply and demand are motivating changes in this system; this ongoing

Smart-Grid Security Issues

The North American electric power grid is a highly interconnected system, considered by many as one of the 20th century's greatest engineering feats. Still, changing power supply and demand are motivating changes in this system; this ongoing modernization is often called the "smart grid". This process has many dimensions, such as reliability and efficiency, and many potential benefits—for example, minimizing delivery infrastructure, information security, and smart meters, and smart energy sources such as geothermal and wind power, and increased consumer participation. However, these representations will incur increased risk. Some risk will be tied to tighter integration of the digital communications and computer infrastructure with the existing physical infrastructure, with all the inherent vulnerabilities. Other risk comes from changes in how power companies and consumers interact. Here we describe some known changes and highlight security issues related to the infrastructure digital domain.

A Look at Smart Grids

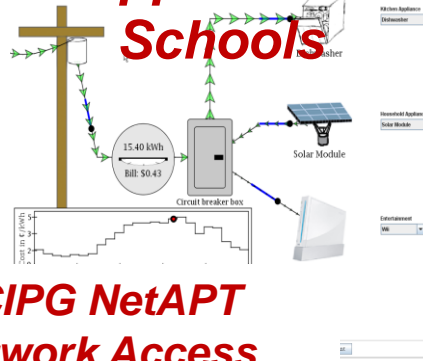
The smart grid (Fig. 1) uses intelligent transmission and distribution networks to deliver electricity. This approach aims to improve the electric system's reliability, security, and efficiency through the use of intelligent communication of consumption data and dynamic optimization of electric system operations, maintenance, and planning.



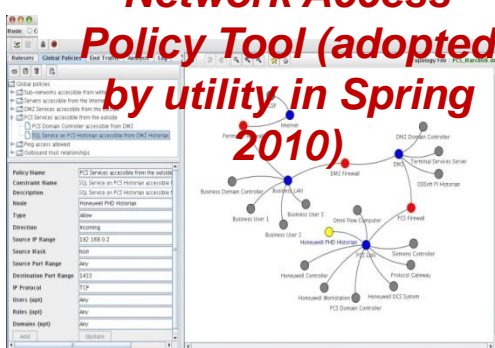
Recent Papers



Applets for Schools



TCIPG NetAPT Network Access Policy Tool (adopted by utility in Spring 2010).



Funding

\$18.8 million over 5 years (2009-2014)

from DOE and DHS

Facilities

Test bed combining power grid hardware and software with sophisticated simulation and analysis tools

Game-changing R&D Needed to Make Survivable Systems a Reality

University of Illinois • Dartmouth College University of California at Davis • Washington State University

DOE National SCADA Test Bed (NSTB)

System Vulnerability Assessments - SCADA/EMS

- Completed assessments of 38 vendor control systems and associated components on-site at utility field installations and at the INL SCADA Test Bed facility



Detroit Edison



TELVENT

AREVA

SIEMENS



ABB



GE Energy



OSIsoft.



OSI

opening your world

NSTB Industry Outreach: Vendors, Asset Owners

Objective: Share information with industry related to cyber vulnerabilities and mitigations

Approach: Provide value to industry groups and initiatives who's goal is to improve the cyber security posture of control systems for the Energy Sector

Progress/accomplishments: Provided awareness training for over 4,000 people through Red/Blue Team Advanced training workshops (+180 trained) other training sessions (+400 hands-on), events and conferences

Benefits: Increasing vendor and user awareness related to vulnerabilities and mitigations. Learn from the asset owners the issues and problems associated with mitigating cyber security vulnerabilities. Common Vulnerabilities and lessons cyber exercises shared. Provide awareness for energy sector stakeholders (asset owners, vendors, government, industry organizations, etc.)



2010 Industry-Led DOE-OE DOE CEDS Projects

Telcordia Cybersecurity for Energy Delivery Systems Communications Protocols: Research energy-sector communication protocol vulnerabilities, and develop mitigations that harden these protocols against cyber-attack and that enforce proper communications within energy delivery systems. Lead: Telcordia Technologies Partners: University of Illinois, Electric Power Research Institute (EPRI), DTE Energy

Grid Protection Alliance: Secure Information Exchange Gateway: Research, develop and commercialize a Secure Information Exchange Gateway that provides secure communication of data between control centers. Lead: Grid Protection Alliance Partners: University of Illinois, Pacific Northwest National Laboratory, PJM, AREVA T&D

Sypris Cryptographic Key Management for AMI: Research, develop and commercialize a cryptographic key management capability scaled to secure communications for the millions of smart meters within the Smart Grid Advanced Metering Infrastructure. Lead: Sypris Electronics Partners: Purdue University Center for Education and Research in Information Assurance and Security (CERIAS), Oak Ridge National Laboratory (ORNL), Electric Power Research Institute (EPRI)

SEL Padlock: Research, develop and commercialize a low-power, small-size dongle that provides strong authentication, logging, alarming and secure communications for intelligent field devices operating at the distribution level. Lead: Schweitzer Engineering Laboratories (SEL) Partners: Tennessee Valley Authority (TVA), Sandia National Laboratories (SNL)

2010 Industry-Led DOE-OE DOE CEDS Projects (continued)

SEL WatchDog Managed Switch: Research, develop and commercialize a managed switch for the control system local area network (LAN) that uses whitelist filtering and performs deep packet inspection. Lead: Schweitzer Engineering Laboratories (SEL) Partners: CenterPoint Energy Houston Electric, Pacific Northwest National Laboratories (PNNL)

SEL Whitelist Antivirus: Research, develop and commercialize a whitelist antivirus for control systems solution to be integrated with Schweitzer Engineering Laboratories substation-hardened computers and communication processor. Lead: Schweitzer Engineering Laboratories (SEL) Partners: Dominion Virginia Power (DVP), Sandia National Laboratories (SNL)

Siemens Energy Cyber-Physical System Security Status: Develop and demonstrate a near-real-time cyber and physical security situational awareness capability for the control system environment. Lead: Siemens Energy, Inc. Partners: Sacramento Municipal Utilities District, Pacific Northwest National Laboratories Advisors: CenterPoint Energy, Omaha Public Power District, New York Power Authority

Honeywell RBAC with Least Privilege: Research, develop and commercialize a role-based access control (RBAC) –driven, least privilege architecture for control systems. Lead: Honeywell International, Inc. Partners: University of Illinois, Idaho National Laboratory

2010 Laboratory-Led DOE-OE DOE CEDS Projects

High-Level (4th Gen) Language Microcontroller Implementation - Idaho

Limits direct access to device memory

Hardens microcontrollers against low-level cyber-attacks (such as buffer overflow)

Develop standardized security library to implement secure authentication and data encryption down to the hardware level

Partners: Siemens Corporate Research

Control System Situational Awareness Technology Interoperable Tool Suite - Idaho

Shows all control system network communications taking place (Sophia);

Collects all wireless mesh network data message routes;

Reports unexpected behavior (Mesh Mapper);

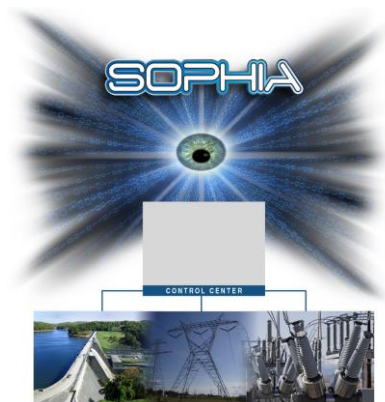
Monitors system health;

Distinguishes between component failure and cybersecurity incidents (Intelligent Cyber Sensor);

Performs data fusion for situational awareness (Data Fusion System);

Determines global effects of local firewall rules (NetAPT)

Partners: Idaho Falls Power, Austin Energy, Argonne National Laboratory, University of Illinois, Oak Ridge National Laboratory, University of Idaho



2010 Laboratory-Led DOE-OE DOE CEDS Projects (continued)

Automated Vulnerability Detection For Compiled Smart Grid Software – Oak Ridge

Performs static analysis of compiled software and device firmware

Partners: Software Engineering Institute (SEI), The University of Southern Florida (USF), EnerNex Corporation

Next Generation Secure, Scalable Communication Network for the Smart Grid – Oak Ridge

Uses adaptive hybrid spread-spectrum modulation format

Provides superior resistance to multipath, noise, interference and jamming

Appropriate for high quality-of-service (QoS) applications.

Partners: Pacific Northwest National Laboratory (PNNL), Virginia Tech, OPUS Consulting, Kenexis Consulting

Bio-Inspired Technologies for Enhancing Cybersecurity in the Energy Sector – Pacific Northwest

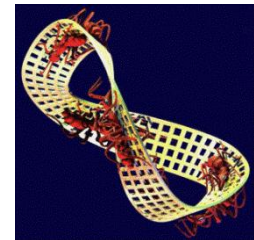
Across multiple organizational boundaries found in Smart Grid architectures

Uses *Digital Ants* - many lightweight and mobile agents whose activities

Correlates to produce emergent behavior

Draws attention to anomalous conditions--potentially indicative of a cyber-incident

Partners: Wake Forest University, University of California-Davis, Argonne National Laboratory (ANL), SRI International



For more information ...

Contact:

US Department of Energy

Carol Hawk

Carol.Hawk@hq.doe.gov

202-586-3247

Diane Hooie

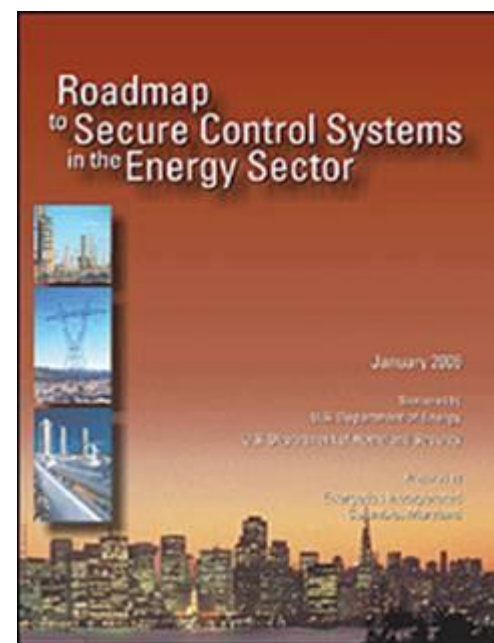
Diane.Hooie@netl.doe.gov

304-285-4524

Visit:

www.oe.energy.gov/controlsecurity.htm

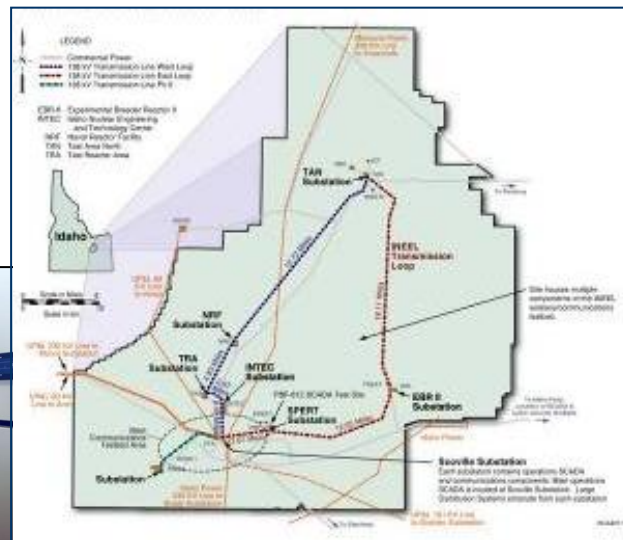
www.controlsystemsroadmap.net



Critical Infrastructure Test Range Complex

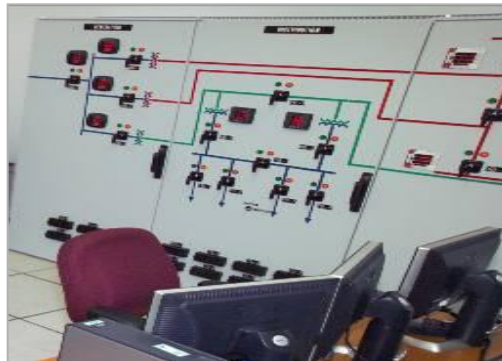
Power Grid and Communications - Idaho

- **Secure power distribution system**
 - 61 mi dual 138 kV power loop
 - 7 substations with 3 commercial feeds
- Ability to isolate portions of grid/substation
- Centralized SCADA operations center
- Power line test area
- Real Time Digital Simulator
- **Traditional Phone Networks**
- **Ethernet**
- **Next Generation Cellular**
- **Wireless networks**
- **Manage spectrum**



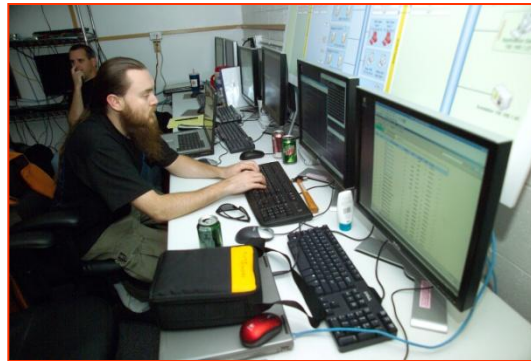
Critical Infrastructure Test Range Complex - Control Systems Idaho

- Legacy Architectures
- Non-production configurations
- Latest versions from Vendor Partners
- Emulators/simulators
- Connectivity to other CITRC assets



Cyber Security of Control Systems - Idaho

- Cyber Security Assessments on Control Systems
- Zero Day (New) Exploits
- Protocol Analysis
- Partial Code Review and Reverse Engineering
- Component Firmware and Embedded Devices
- Wireless Security
- IDS Review, Testing, Configuration and Design
- Forensics Review and Malware Analysis
- Controlled Information Sharing and Demonstrations
- Security Training / Outreach



DHS National Cyber Security Division

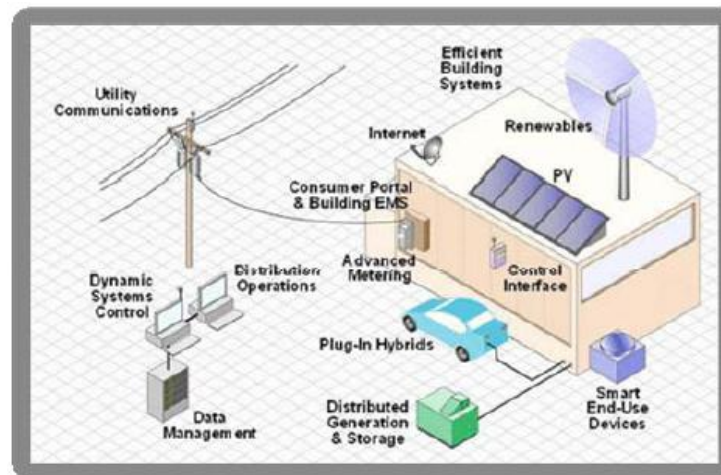
Control Systems Security Program



www.us-cert.gov/control_systems

Electric Distribution Smart Grid Applications

- Two Way Communications Networks for status and control
 - Transmission – better situational awareness
 - Generation – ability to add intermittent renewable generation
 - Distribution – manage distribution load - Billing, Outage Management
- Distribution: Advanced Metering Infrastructure (AMI) will install smart meters on residential, commercial and industrial
 - Remote connect and disconnect
 - Normally wireless to residences
- Physical Access an issue with wireless access points in neighborhoods



Source: Department of Energy

Vulnerability Discovery, Exploits and Consequences AMI

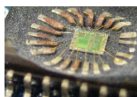
- Vulnerability Discovery
 - Low barrier of entry to meters and networks for vulnerability discovery and exploitation
- Exploits
 - Being written and already exist prior to smart grid – e.g. wireless
- Consequences
 - Propagating Malware
 - Financial

Travis
Goodspeed:
A 16-bit Rootkit
and Second
Generation Zigbee
Chips

Vulnerabilities, Exploits and Consequences Observed

AMI Embedded Systems

- Insecure data busses and serial connections
 - C12.22 bus
 - Data Capture, Injection (both directions)
 - Radios
 - MCU's
- Stealing/Replacing Keys In Memory
 - Network Encryption
 - Authentication and CA keys
- Blown JTAG Fuse Isn't Enough
 - Third-party labs remove top/allow microscopic access to chip
- Firmware-level vulnerabilities similar to x86 systems
- It's the Latch!



ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM



ICS-CERT ADVISORY

ICSC-09-348-01-A - INTELLICOM NETBITER® WEBCADA VULNERABILITY UPDATE
January 13, 2010

INFOZ

Who:	Hackers Like You.
What:	ToorCon 11
When:	OCT 23rd-25th
Where:	San Diego Convention Center
Why:	What Could possibly go wrong?

Home • Conference • Talks • KillerBee: Practical ZigBee Exploitation Framework

KillerBee: Practical ZigBee Exploitation Framework

ZigBee is a vital component of several emerging technologies including smart grid systems, bridging the devices in your home with the electric utility. With the rush to deploy this technology, few organizations have examined the security threats in this suddenly "critical infrastructure" wireless protocol.

Over the past 9 months, the speaker has been assessing various implementations of ZigBee technology while building a tool suite designed to exploit these networks. In this talk, the author will present several findings regarding the vulnerabilities in ZigBee networks, releasing the KillerBee attack framework designed to exploit ZigBee networks.

Joshua Wright

Case Study – Fraud

POWER THEFT

If you wish to report any suspicious activity you press the link below to access the online form [Theft of Energy](#) .

The Cost of Energy Theft

Each year, the Power Authority lost more than \$ 400 million as a result of **theft of** electricity in Puerto Rico. When steals energy cost is transferred to honest customers. Like any other business, the economic losses **of Energy Theft** operational costs increase. These costs alone are high without adding the aggravating circumstance of robbery.

Threat to Security

Energy Theft is a safety hazard, electrical shock, property damage involve the thief, but the innocent Authority.

Informants include the full name on the form can be contacted by ESA to serve as witnesses in the investigation of cases.

Contact the Authority, if you see one of the following situations:

- When a person who is not identified as an employee of the Electric Power Authority, spoke with an accountant or the basis of a counter.
- When a person who is not employed by the Power Authority, working near underground lines or airlines of the ESA.
- If you hear someone comment on how little you pay for electricity from speaking the counter or get a "power saver".
- Use unbridled energy.

Notifies any suspicious activity related to an accountant. Call us at **1-866-664-8783 (1-866-No Hurt)**, the Customer Service Center 787-521-3434 or visit one of our Customer Service Office.

Complex Networks and Standards Issues

Networks

- New networks on networks schemes are complex to defend
- Increased dependence on utility's wireless communications
- Ownership of data communications and cyber security for power (Base or Municipality vs. Utility)

Standards

- Different security standards NIST; NERC CIP, Zigbee Alliance, IEC, IEEE C12.10, DoDI 8500.2



AMI System Security Requirements

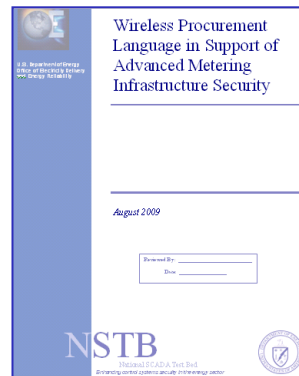
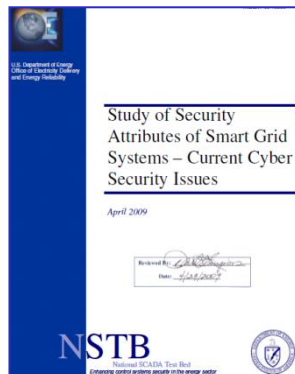
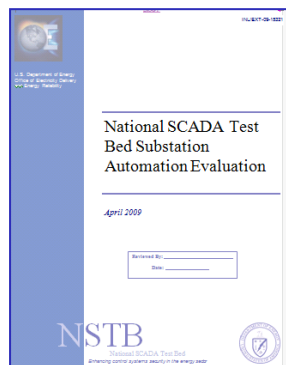
V1.01

ASAP

12/17/2008

Executive Summary

This document provides the utility industry and vendors with a set of security requirements for Advanced Metering Infrastructure (AMI). These requirements are intended to be used in the procurement process, and represent a superset of requirements gathered from current cross-industry accepted security standards and best practice guidance documents.



Security Check and Balance Considerations

- Know the Business
 - Coupled or de-coupled rate structures
- Know the Customer Profile
 - Support green energy, price conscience, aware of energy efficiency, hostile or disinterested
- Quality Assurance Checks on Meter Reads
 - At installation, after upgrades, and spot checked periodically
- Revenue Protection Applications
 - Query to meter data management databases for out of bounds
 - Vacation homes, local and private generation
 - Power accounting from distribution substation to neighborhood load – accuracy of substation meters



Recommendations: Incorporating Security

- Start at the beginning of the life cycle
- Proactively require vendors, technology providers and integrators for security assurances and features
- Design in checks and balances
- Third party validation of security measures
- Continuous verification of security measures

Thank You

Rita Wells
Rita.wells@inl.gov
(208) 526-3179